Axe Infini

Algorithmics for symbolic verification of infinite systems

Alain FINKEL

Plan

1. **Introduction**
    1. Scientific context
    2. Forward reachability procedure
    3. Backward reachability algorithm
    4. Our two preferred models

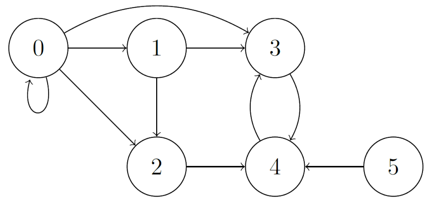
2. WSTS and CM

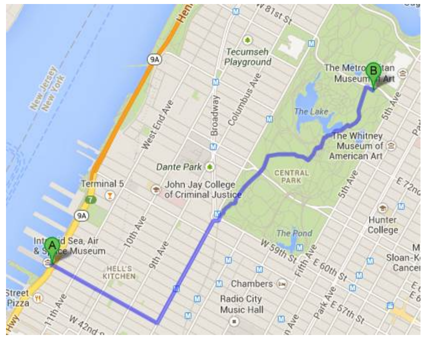
3. Management

4. 5 Strategy

Scientific context

- What objectives do we address ?
  - Automatic analysis of (abstraction of) programs with unbounded parameters (stack, channel, recursive,…).
  - Analyse = solve reachability from s towards t
  - Analyse = ∃ path s --*→ t in an infinite graph ?
  - Needs finite and computable representations

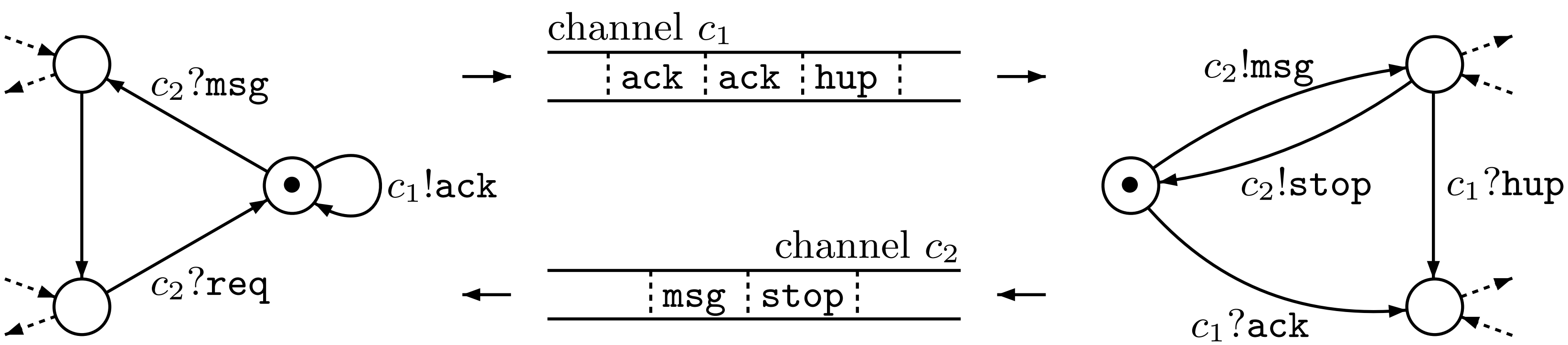




Communicating programs

finite control but unbounded channels

unbounded



unbounded

Lists program

is this program correct ?

```
List Reverse (List x)  {
 List y,t;
 y= NULL;
 while (x!=NULL) {
   t=y;
  y=x;
  x=x->n;
  y=n->t;
  t=NULL;}
 return y;}
```

Recursivity and counter

- From P(17), will R necessarly be activated ?

$$
\begin{array}{l}
P(x)\text{: If } x \geqslant 16 \\
\qquad\qquad \text{If } 8|x \text{ then } Q(x+1) \\
\qquad\qquad \text{else } P(x-2) \\
\qquad \text{else } F(x)
\end{array}
$$

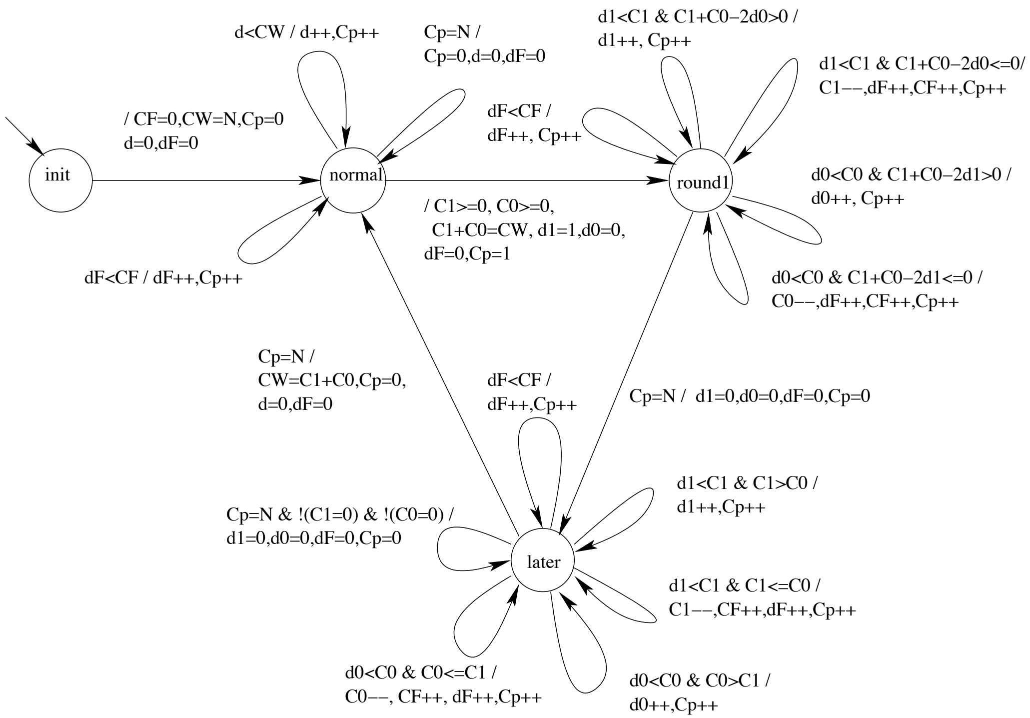
$$
\begin{array}{l}
Q(x)\text{: If } 2|x \text{ then } R(x) \\
\qquad \text{else } S(x+1)
\end{array}
$$

In Bouajjani &al TCS n°295, 2003, page 86

Modelisation of the communication protocol TTP

only +1 and -1 operations but already difficult analysis

Model for the TTP, N stations



Plan

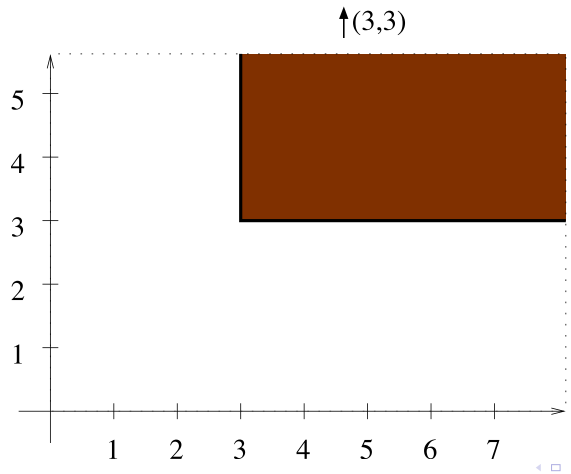
1. **Introduction**
    1. Scientific context
    2. Forward reachability procedure
    3. Backward reachability algorithm
    4. Our two preferred models

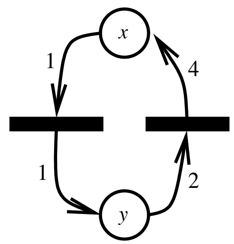
2. WSTS and CM

3. Management

4. 5 Strategy

Reachability is difficult for “simple” CM



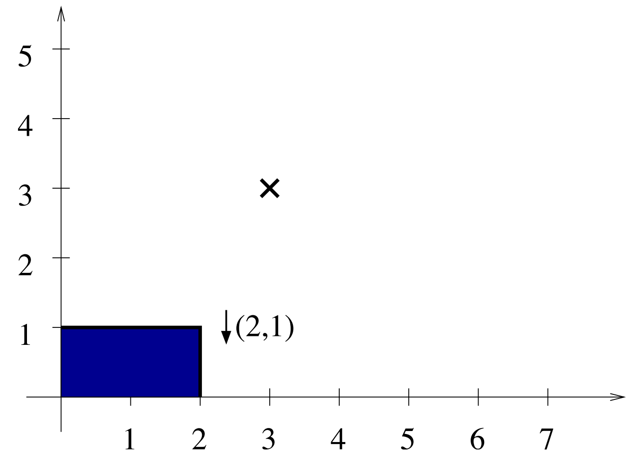


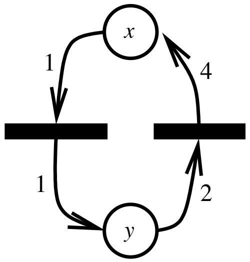
- t_1: (x,y) → (x-1,y+1)
- t_2: (x,y) → (x+4,y-2)

- Is there a path s.t.:

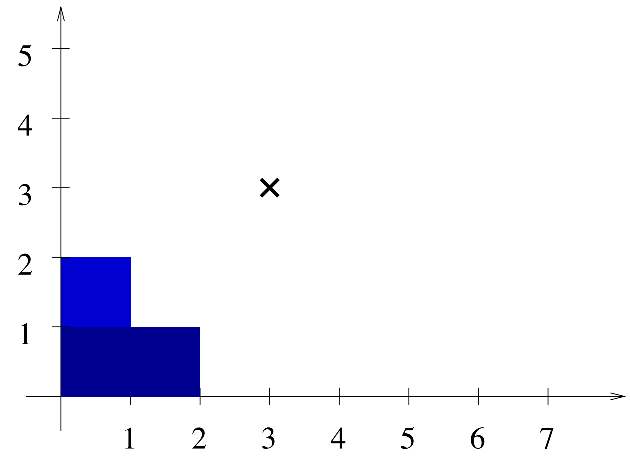
(2,1) →…*… →↑(3,3) ?

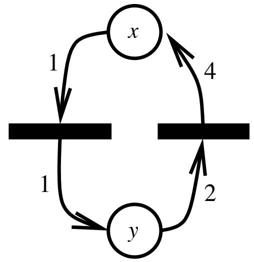
A Naive Forward Algorithm



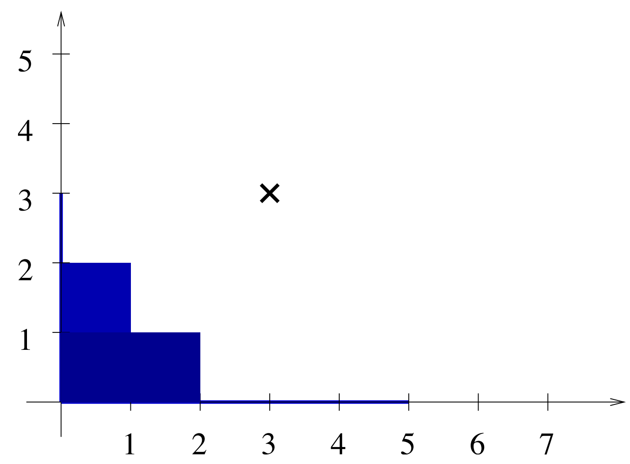


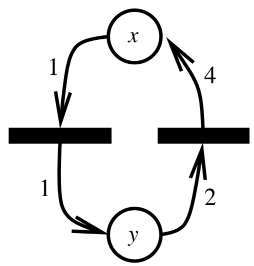
A Naive Forward Algorithm



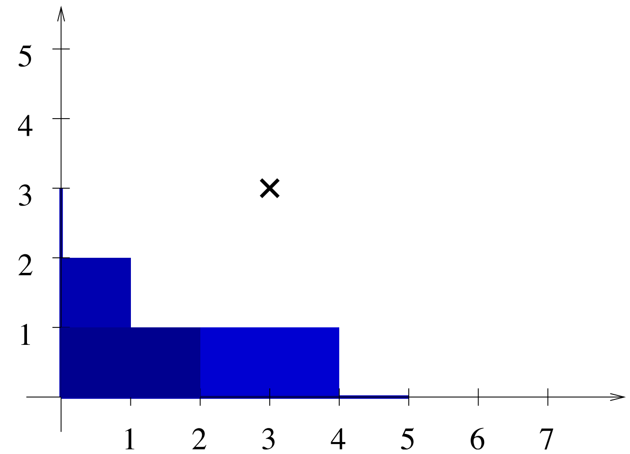


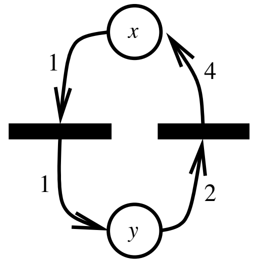
A Naive Forward Algorithm



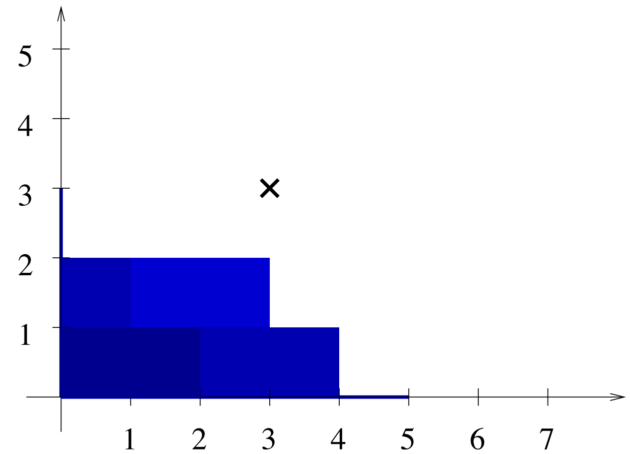


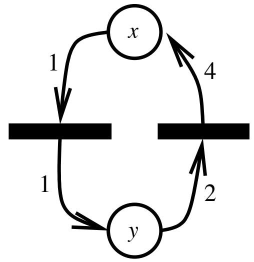
A Naive Forward Algorithm



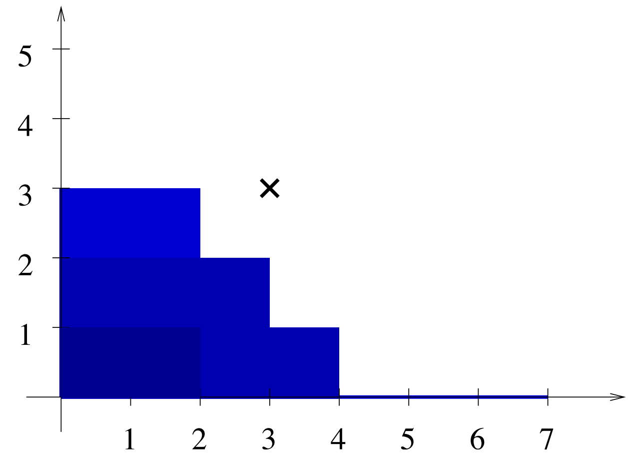


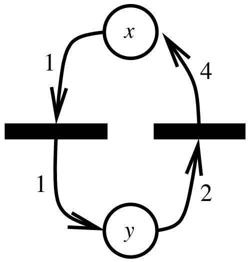
A Naive Forward Algorithm



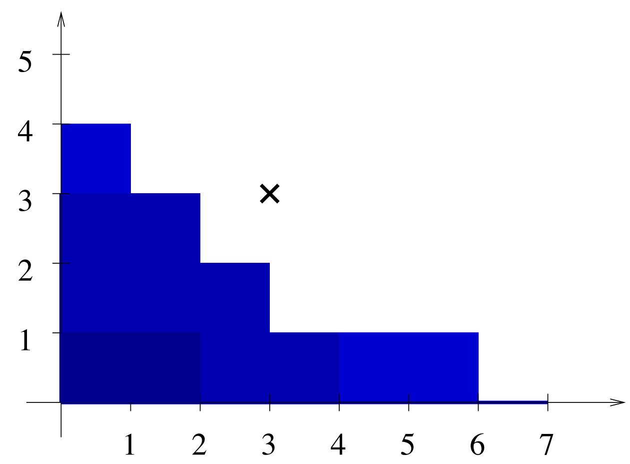


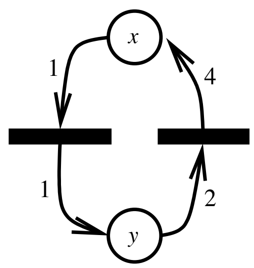
A Naive Forward Algorithm



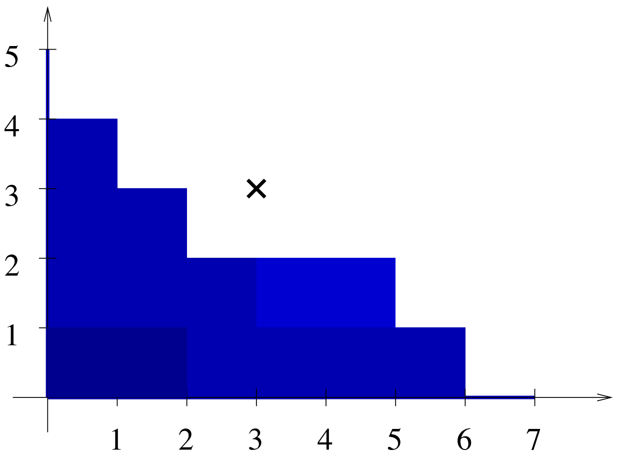


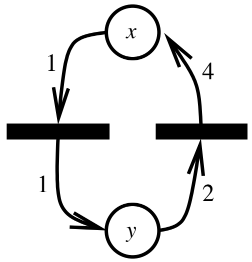
A Naive Forward Algorithm

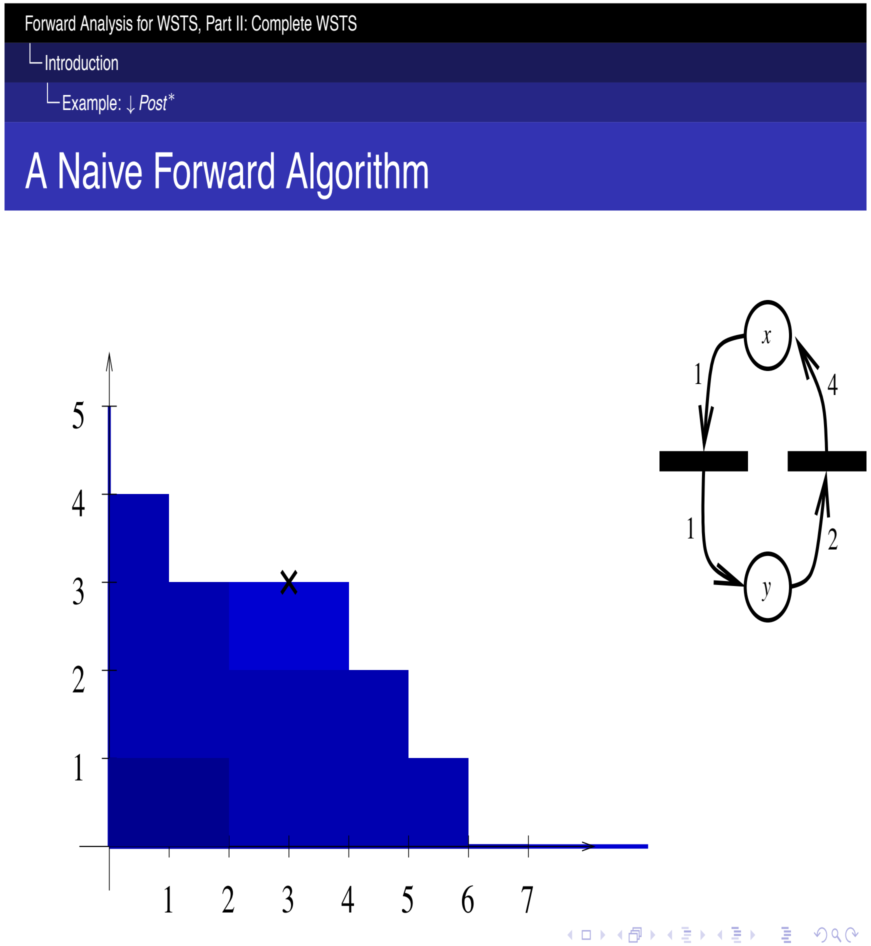




A Naive Forward Algorithm

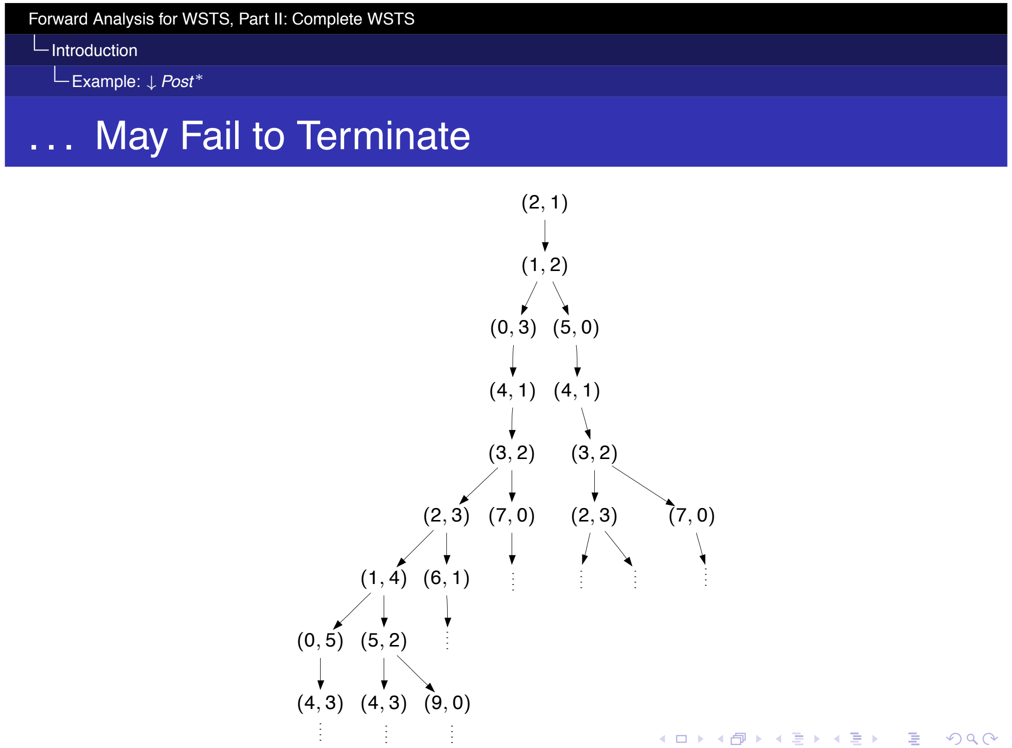






- A path of length 8 from ↓(2,1) which meets (3,3)

Infinite reachability tree



$$
\begin{tikzcd}
& (2,1) \arrow[d] & \\
& (1,2) \arrow[dl] \arrow[dr] & \\
(0,3) \arrow[d] & & (5,0) \arrow[d] \\
(+\infty, 1) \arrow[d] & & (+\infty, 1) \arrow[d] \\
(+\infty, +\infty) & & (+\infty, +\infty)
\end{tikzcd}
$$

Is Post*(2,1) (finitely) computable ?
When does this procedure terminate ?

Plan

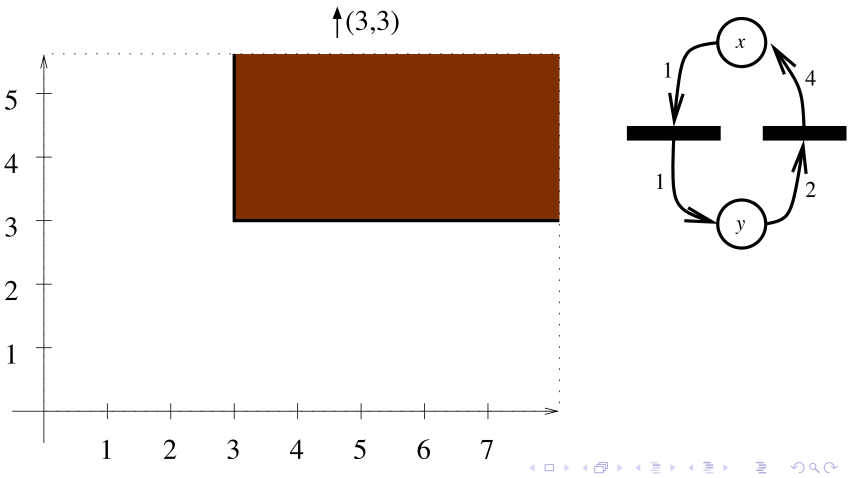
1. **Introduction**
    1. Scientific context
    2. Forward reachability procedure
    3. Backward reachability algorithm
    4. Our two preferred models

2. WSTS and CM

3. Management

4. 5 Strategy

Reachability/coverability

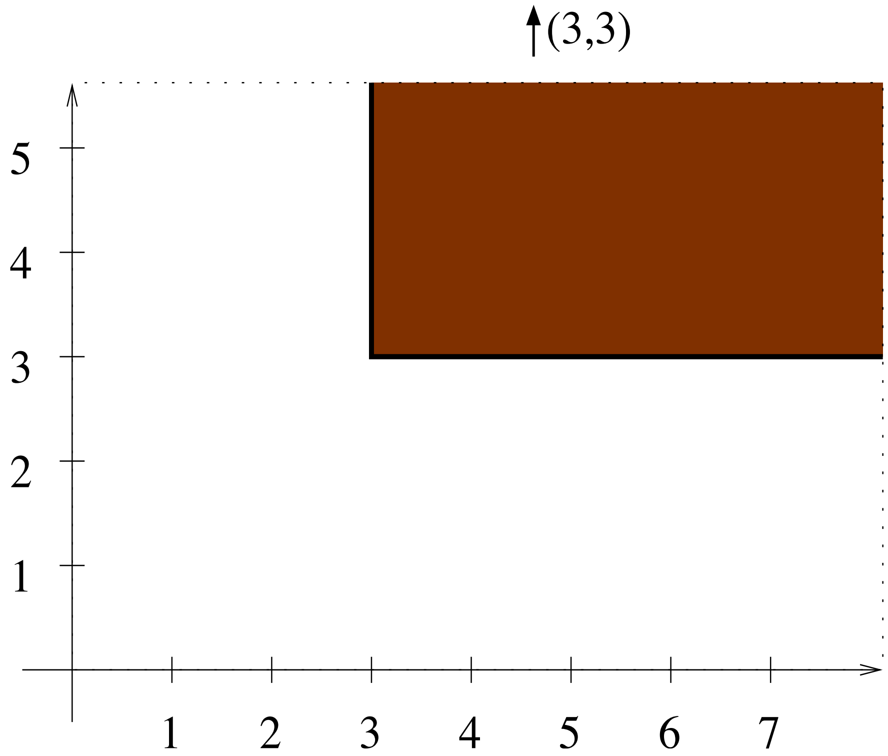


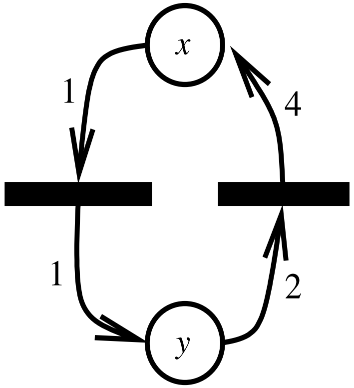
- t_1: (x,y) → (x-1,y+1)
- t_2: (x,y) → (x+4,y-2)

- Is there a path s.t.:

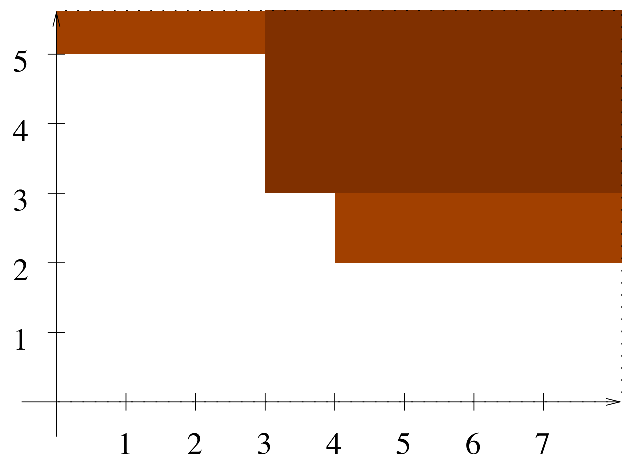
(2,1) →… → ... → ↑(3,3)

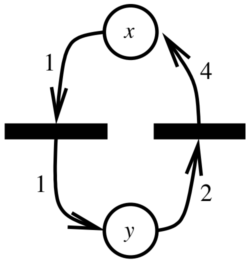
Example: Coverability (in Petri Nets, here)



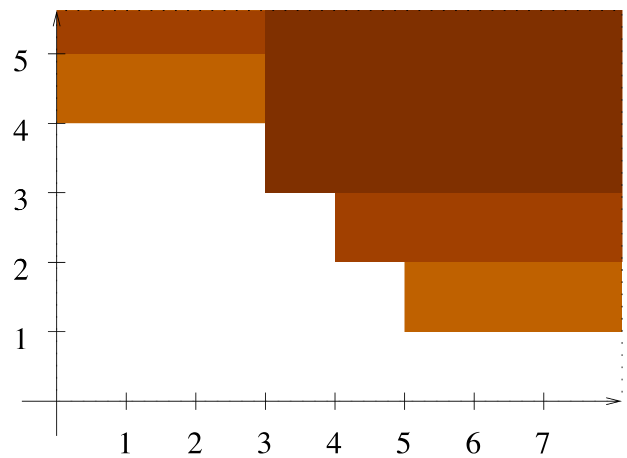


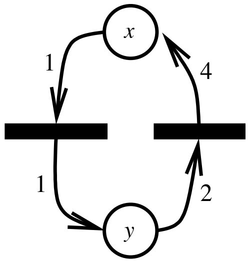
Example: Coverability (in Petri Nets, here)



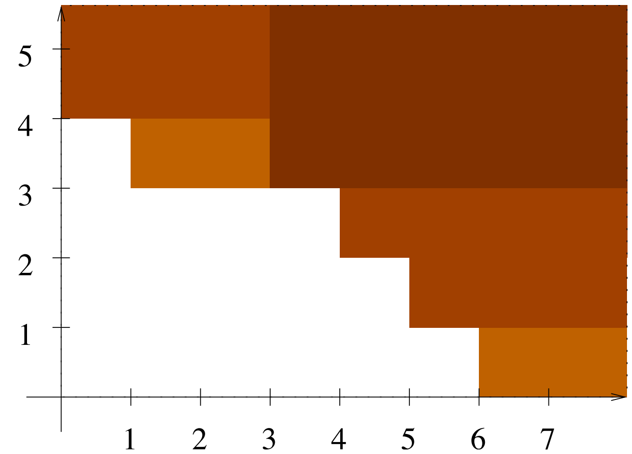


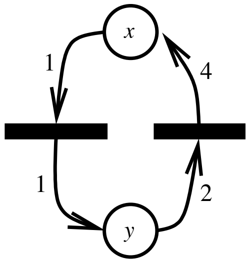
Example: Coverability (in Petri Nets, here)



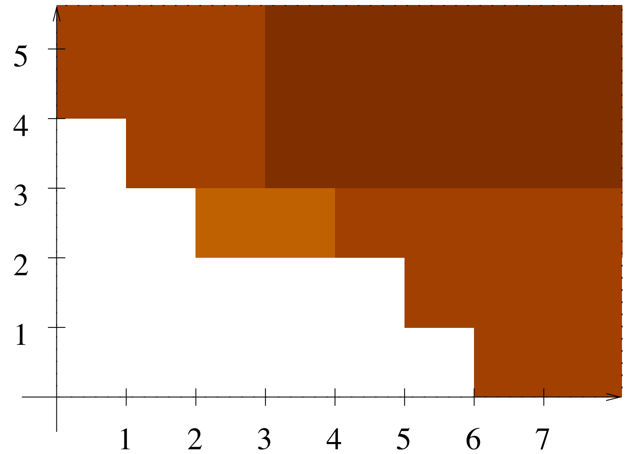


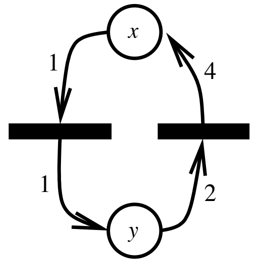
Example: Coverability (in Petri Nets, here)



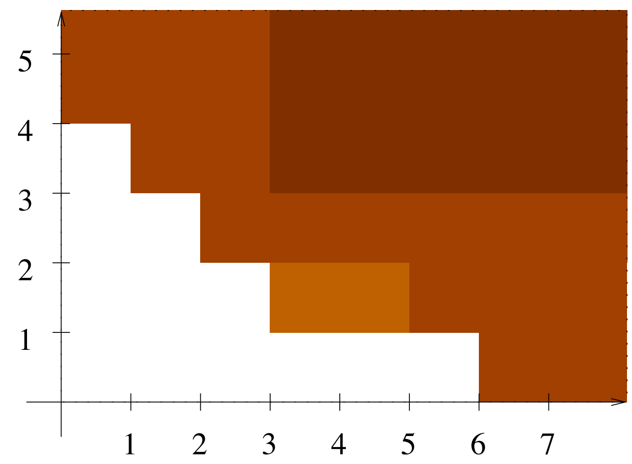


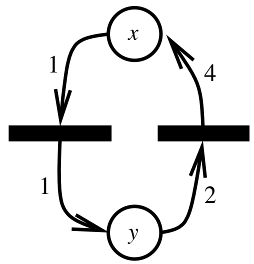
Example: Coverability (in Petri Nets, here)



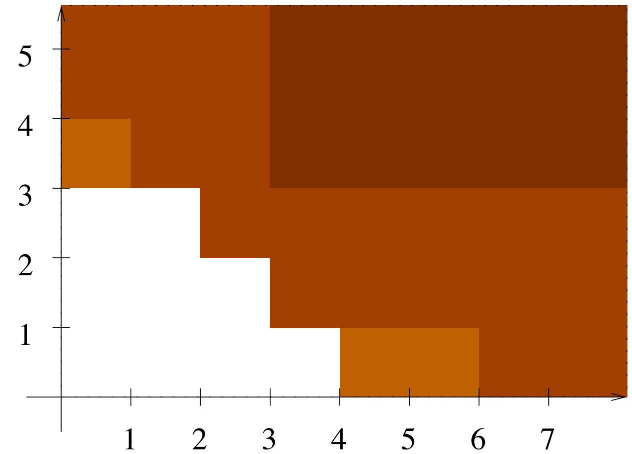


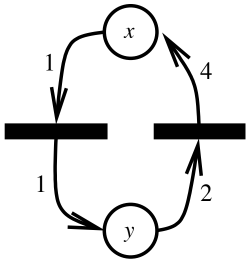
Example: Coverability (in Petri Nets, here)



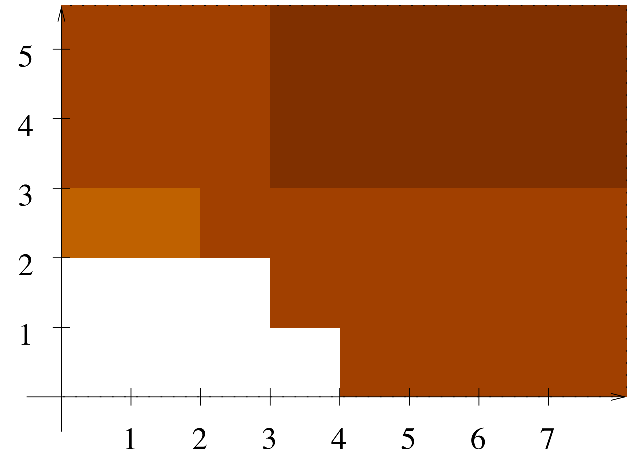


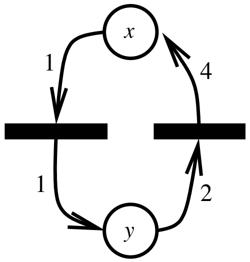
Example: Coverability (in Petri Nets, here)



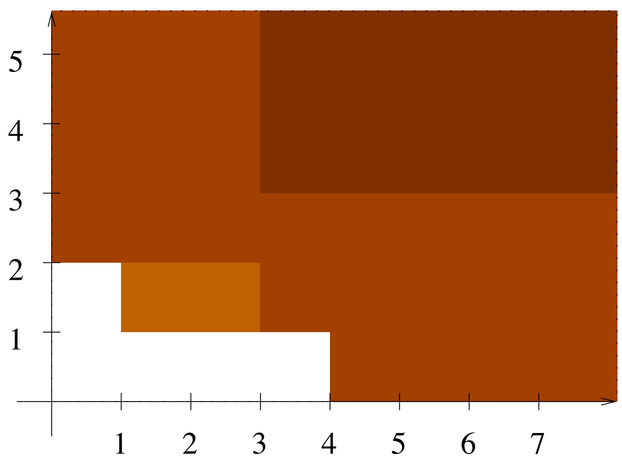


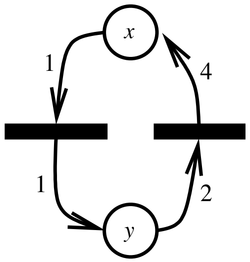
Example: Coverability (in Petri Nets, here)



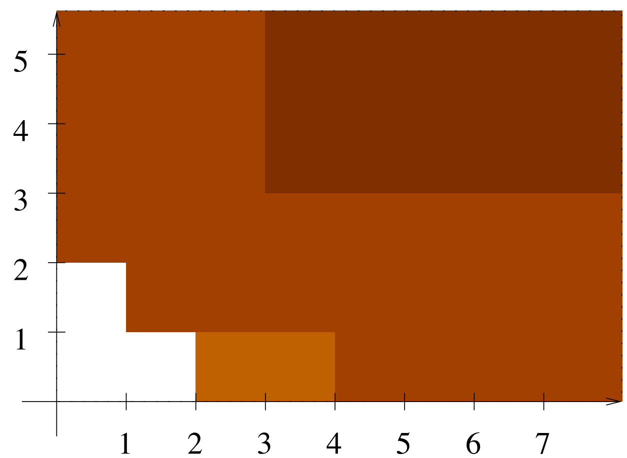


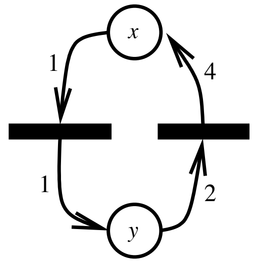
Example: Coverability (in Petri Nets, here)



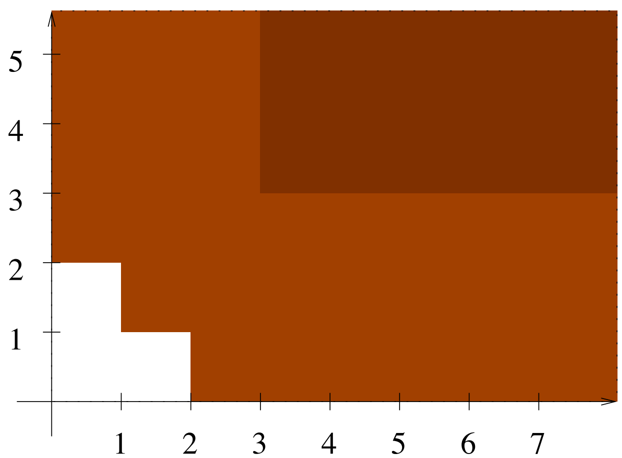


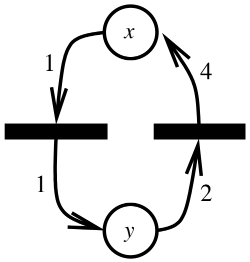
Example: Coverability (in Petri Nets, here)





Example: Coverability (in Petri Nets, here)





Backward strategy

- A path of length 10 from ↑ (3,3) that finally contains state (2,1).

Plan

1. **Introduction**
    1. Scientific context
    2. Forward reachability procedure
    3. Backward reachability algorithm
    4. Our two preferred models

2. WSTS and CM

3. Management

4. 5 Strategy

Our two preferred models

- WSTS: generic (=abstract) model for tens of « concrete » models

- Counter machines : universel model for computation (& modelization/verification)

Well Structured Transition Systems (WSTS)

- Ingredients:
  - A transition relation $\delta \subseteq X \times X$;
  - A well quasi-ordering (wqo) $\leq$ on X;
  - + monotonicity:

$$\begin{tikzcd} x \arrow[r, "\leq"] \arrow[d, "\delta"'] & x' \arrow[d, dotted, "\delta"] \\ y \arrow[r, dotted, "\leq"] & y' \end{tikzcd}$$

- $\leq$ is wqo iff (equivalently):
  - no infinite descending chain, and no infinite antichain;
  - every sequence has an infinite non-decreasing subsequence;
  - every upward-closed subset U is of the form $\uparrow A$, A **finite**.

WSTS and WQO history

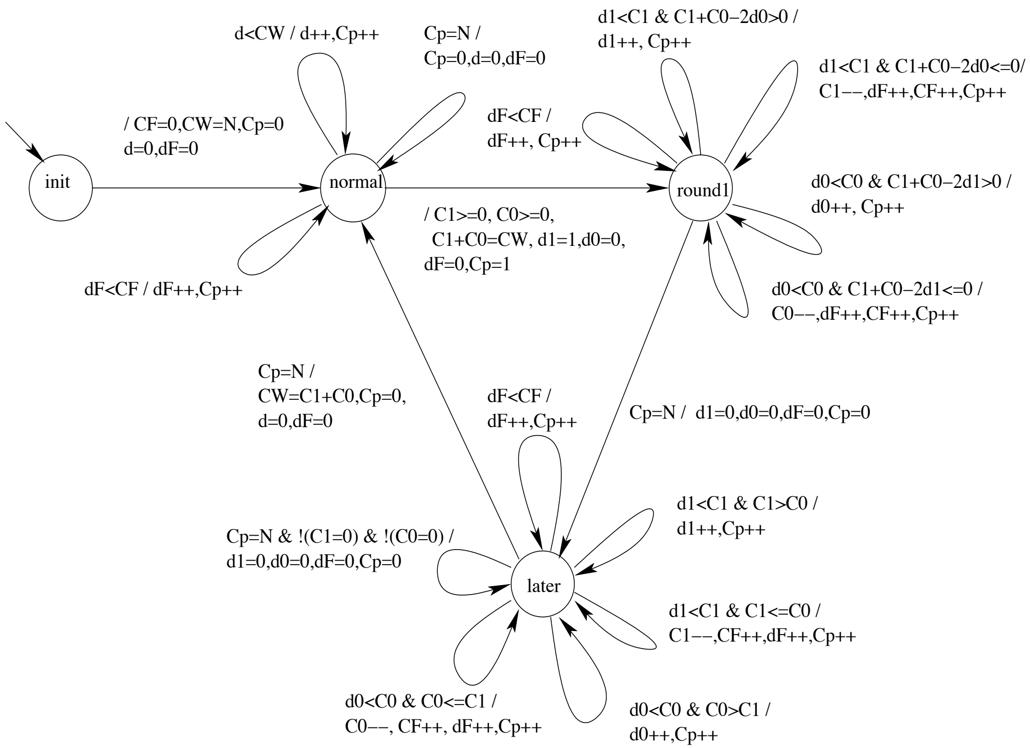
- Timeline
  - ICALP 1987 : basis of the theory
  - TCS 2001 : survey of the theory
  - IPL 2002: Reachability is non Recursive Primitive
  - STACS 2009 + ICALP 2009: mathematical fundations to forward analysis
  - LICS 2008
  - MFCS 2010
  - LICS 2011
  - ESSLLI 2012
  - LICS 2012
  - Petri 2011, Petri 2012
  - CONCUR 2013

Complexity & decidability of WSTS

- Success : used and studied by numerous colleagues (Henzinger, Raskin,…)

Counter Machines (CM)

Model for the TTP, N stations



Plan

1. **Introduction**
    1. Scientific context
    2. Forward reachability procedure
    3. Backward reachability algorithm
    4. Our two preferred models

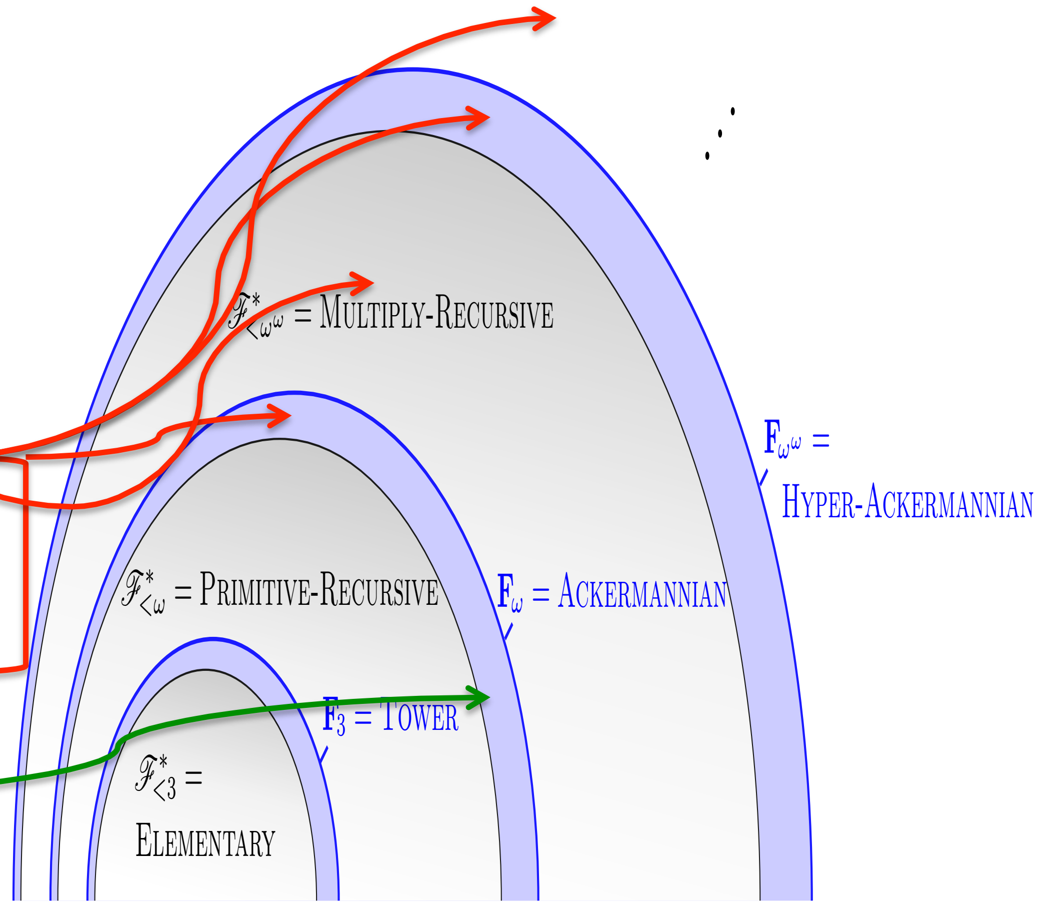
2. **WSTS and CM**
    1. Highlight: wqos and complexity
    2. WSTS
    3. Counter Machines

3. Management

4. Strategy

Highlight : complexity of WQO

- Jancar TCS'01
  The finite reachability set equality for Petri nets
- **Schnoebelen IPL'02**
  Reachability LCS
- Reachability LCM (MFCS 2010)



Highlight : complexity of WQO

Challenges: Complexity of WSTS

- Concepts for measuring length of wqo (done)
- Upper/lower bounds (beginning)
- Publications LICS 2008, MFCS 2010, LICS 2011, FOSSACS 2011, ICALP 2011, LICS 2012, MFCS 2013

Projects 2013-2017

- Delineate models/problems
- Equivalences/hierarchy
- Towards a Garey & Johnson of non-elementary complexities

Plan

1. **Introduction**
    1. Scientific context
    2. Forward reachability procedure
    3. Backward reachability algorithm
    4. Our two preferred models

2. **WSTS and CM**
    1. Highlight: wqos and complexity
    2. WSTS
    3. Counter Machines

3. Management

4. Strategy

A paradox ?

- Backward strategy always terminates but is not efficient.
- The tool Trex (LIAFA) does not use the backward algorithm

No paradox

Forward is more efficient than backward

- Backward strategy always terminates but is not efficient.
- Accelerated forward strategy often terminates with efficiency but no theory

- The tool Trex (LIAFA) does not use the backward algorithm
- Trex uses an adhoc accelerated forward procedure without termination guarantee

No theory of downward closed sets

Upward closed sets

- A nice and simple theory

- **Theorem** (~1900)

For all $X \subseteq A$, A wqo,

$\uparrow X = \uparrow\{x_1, x_2, \ldots, x_n\}$ with $x_i \in X$.

Downward closed sets

- Missing theory

"Finally, we aim at developing generic methods for building downward closed languages, …. This would give a general theory for forward analysis of infinite state systems, in the same way the work is for backward analysis." Abdulla & [FORMATS 2004]

- **Open problem** (2008)

For all $X \subseteq A$, A wqo, is $\downarrow X$ finitely descriptible ?

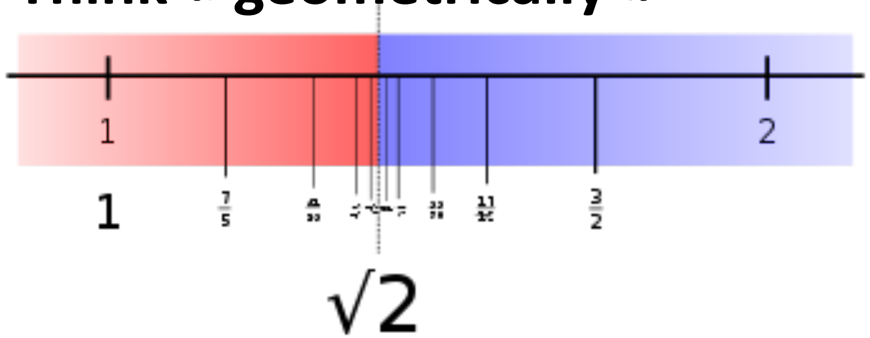
We have : $\downarrow X \neq \downarrow \{x_1, x_2, \ldots, x_n\}$ with $x_i \in X$

Towards a theory of downward closed sets

Mathematical and cognitive hypothesis

- limits are points at infinity but it does not work well
- Need of a « new » paradigm of limits which allows representing infinite downward closed sets.

Think « geometrically »

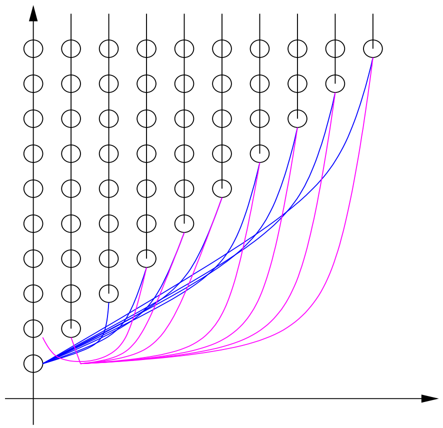


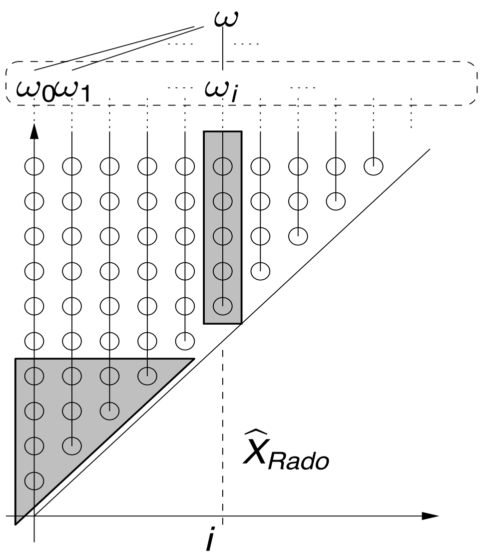
Think « algebraically »

- Identify $x \in X$ with the subset $\downarrow x \subseteq X$
- Elements and limits are directed downward closed subsets (= ideals)
- Theorem (STACS 2009)

$\downarrow X = \{I_1, I_2, \ldots, I_n\}$

where I_i are ideals.





WSTS: challenges and results

2008 WSTS Challenges

- Build an unified general theory of forward analysis
- Simplify algorithms + proofs
- Mesure the complexity

Results: 2008 - 2013

- Built a theory of downward closed sets
- Define Complete WSTS
- Define Completion of WSTS
- Conceptual & simple Karp&Miller algo
- Mesure the complexity (highlight)
- Publications: STACS 2009, ICALP 2009, FOSSACS 2011, PETRI 2011, PETRI 2012

Results and projects

Results 2008 - 2013

- Build a theory of downward closed sets in wqo
- Complete WSTS
- Completion of WSTS
- Conceptual Karp&Miller algo
- Publications: STACS 2009, ICALP 2009, FOSSACS 2011, PETRI 2011, PETRI 2012

Projects 2013 - 2017

- Discover the good data-structures for ideals and completion-based algorithms
- Complexity of completion-based algorithms
- Ex: Priority channel systems

Plan

1. **Introduction**
    1. Scientific context
    2. Forward reachability procedure
    3. Backward reachability algorithm
    4. Our two preferred models

2. **WSTS and CM**
    1. Highlight: wqos and complexity
    2. WSTS
    3. Counter Machines

3. Management

4. Strategy

Counter Machines

Challenges and results

CM Challenges in 2008

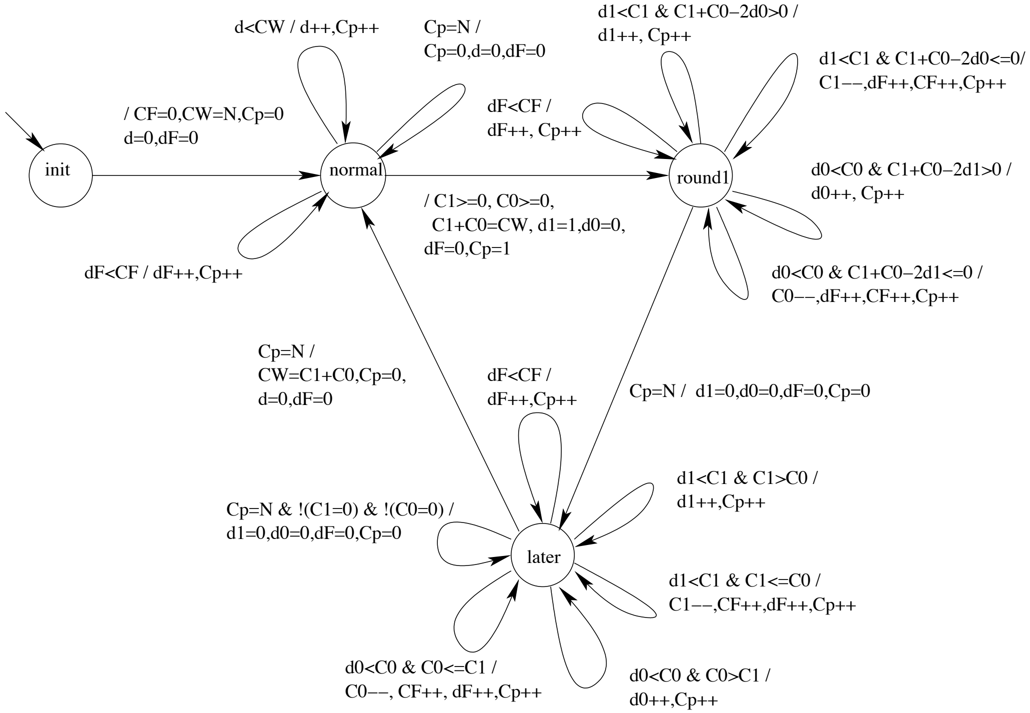
- Unify, extend complexity analysis of Petri nets and classes of CM.
- Complexity of coverability in Petri nets
- Complexity of reachability in Petri nets

CM results 2008 - 2013

- Complexity of logics for Petri nets, flat CM and reversal-bounded CM
- Large classes of "coverability-like" properties are EXPSPACE-complete on Petri nets
- Publications MFCS 2008, MFCS 2010, FSTTCS 2010, FSTTCS 2012, MFCS 2013, ICALP 2013, LICS 2013

Analysis by « simple » subsystems

Model for the TTP, N stations



Results and projects

CM results 2008 - 2013

- Complexity of logics for Petri nets, flat CM and reversal-bounded CM
- Large classes of “coverability-like” properties are EXPSPACE-complete on Petri nets
- Publications MFCS 2008, MFCS 2010, FSTTCS 2010, FSTTCS 2012, MFCS 2013, ICALP 2013, LICS 2013

Projects 2013 - 2017

- Complexity of reachability for Petri nets

  EXSPACE PR ACK

  Multiple-ACK $F_{\varepsilon 0}$

- Complete the book on CMs !
- Towards an algorithmics

Many other subjects…not mentioned

- Games (L. Doyen)
- Lossy channel systems (P. Schnoebelen)
- Parikh automata (with P. McKenzie, Montréal)
- ….

Plan

1. **Introduction**
    1. Scientific context
    2. Forward reachability procedure
    3. Backward reachability algorithm
    4. Our two preferred models

2. **WSTS and CM**
    1. Highlight: wqos and complexity
    2. WSTS
    3. Counter Machines

3. **Management**
    1. Flow of Infini members, PhD, guest post-doc, invited professors
    2. Organization, scientific influence, contracts

4. Strategy

People

December, 2008

- Head : Alain Finkel (Prof. ENS Cachan)
- 3 Permanent members
  - Etienne Lozes (MCF) → Kassel
  - Sylvain Schmitz (MCF)
  - Philippe Schnoebelen (DR CNRS)
- 5 PhD students
  - Florent Bouchy (2006-2009) → Montréal, ing.
  - Rémi Brochenin (DGA/CNRS, 2006-2009) → post doc
  - Jules Villard (2007-2010) → London, post-doc
  - Jean-Loup Carré (EADS, 2007-2010) → Prof classes prépa
  - Pierre Chambart (2008-2011) → Univ. P7, ing.
- Delegations and post-doc
  - Peter Habermehl (MCF Paris7, sabbatical feb.2007-feb. 2009)
  - Pierre-Cyrille Héam (MCF Besançon, sabbatical 2008-2010)
  - Adam Antonik (post-doc)

June, 2013

- Head : Alain Finkel (Prof. ENS Cachan)
- 4 Permanent members
  - Stéphane Demri → New York
  - Laurent Doyen (CR) → Tempo
  - Sylvain Schmitz (MCF) → Dahu
  - Philippe Schnoebelen (DR CNRS)
- 5 PhD students
  - Mahsa Shirmohammadi (Doyen + Massart)
  - Amit Kumar Dahr (Demri + Sangnier)
  - Julien Reichert (Berwanger + Doyen)
  - Prateek Karandikar (Schnoebelen + Kumar)
  - Michael Blondin (F. + McKenzie)
- Chair and post-doc
  - Pierre Mckenzie (Digiteo chair)
  - Christoph Haase (post-doc)

\+ tens of one-month invited professors: Ranko Lazic, Petr Jancar,…

9 PhD students

2008: Arnaud Sangnier (F.+ Lozes) CIFRE EDF	• 2010: Assistant-Prof. Université Paris 7
2009: Florent Bouchy (F.)	• 2013: Post-doc and engineer in Montréal
2009: Jean-Loup Carré (Goubault-Larrecq)	• 2013: Prof Math-sup
2010: Jules Villard (Demri + Lozes)	• 2013: Post-doc Londres
2010: Diego Figueira (Demri + Segoufin)	• 2013: Post-doc Edimbourg
2011: Pierre Chambart (Schnoebelen)	• 2013: Engineer Université Paris 7
2013: Rémi Brochenin (Demri+Lozes)	• 2013: Postdoc University of Genes
2012: Michael Cadilhac (F.+McKenzie)	• 2013: Waiting for a post-doc
January 2013: Rémi Bonnet (F.)	• 2013: Post-doc Oxford (Worrell, Ouaknine)

5 PhD in progress

Mahsa Shirmohammadi (Doyen + Massart)
Markov processes
Defense: 2014

Julien Reichert (Berwanger + Doyen)
Games on counters.
Defense: 2014

Amit Kumar Dahr (Demri + Sangnier)
Flat Counter Machines
Defense: 2015

Prateek Karandikar (Schnoebelen + Kumar)
Lossy Channel Systems & complexity
Defense: 2015

Michael Blondin (F. + McKenzie)
Reachability in Petri nets
Defense: 2016

Plan

1. **Introduction**
    1. Scientific context
    2. Forward reachability procedure
    3. Backward reachability algorithm
    4. Our two preferred models

2. **WSTS and CM**
    1. Highlight: wqos and complexity
    2. WSTS
    3. Counter Machines

3. **Management**
    1. Flow of Infini members, PhD, guest post-doc, invited professors
    2. Organization, scientific influence, contracts

4. Strategy

Organization, scientific influence

- Chairman

GAMES 2011, PaVAS 2011, RP'2012, STSV 2012

- Dagstuhl on infinite systems

april 2014 (Esparza-F.-Mckenzie-Ouaknine)

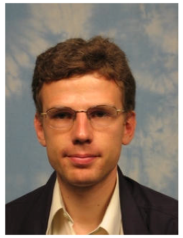
- Publications
  - 33 journal
  - 71 conf

- Collaborations
  - ∞: papiers communs
  - LSV\\∞: Goubault-Larrecq, Haddad,…
  - Monde\LSV: Henzinger, Raskin, Jancar,…

- ANR Blanc « Reachard », LSV/LaBRI (2012-2014)
  - Reachability in VASS and other models
  - http://www.lsv.ens-cachan.fr/Projects/anr-reachard/

Etienne Lozes
(Kassel, Allemagne)
HDR: 3 july 2012

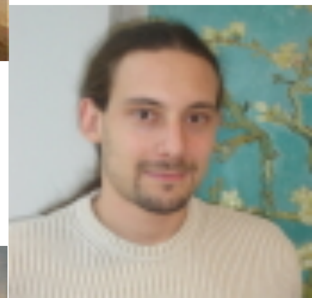
Laurent Doyen
HDR: 13 march 2012

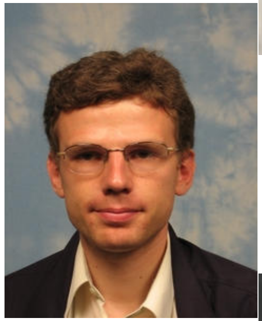


- ANR « DYNRES » (2011-2013)
  - logics for ressources
  - http://anr-dynres.loria.fr/

- + 8 contracts (finished)

December, 2nd, 2013





1. Stéphane Demri
   Dahu - infini
   Marie Curie New York (2012 - 2014)

2. Alain Finkel

3. Sylvain Schmitz
   MCF (2008 -->)
   --> Dahu INRIA (2013-2015)

4. Philippe Schnoebelen

5. Laurent Doyen
   CR CNRS (2009 -->)
   --> Tempo (sept'13 -->)

6. Pierre McKenzie
   Univ. Montréal
   Chaire DIGITEO ENS Cachan-Ecole X
   2013 – 2014

Plan

1. **Introduction**

2. **WSTS and CM**
   1. Highlight: wqos and complexity.
   2. WSTS
   3. Counter Machines

3. **Management**
   1. Flow of Infini members, PhD, guest post-doc, invited professors
   2. Organization, scientific influence, contracts

4. **Strategy**

Check the work of Infini…

Did Infini realize its 2008 objectives ?

From 2008 … to 2013

Perspectives 2008-2013
(AERES, dec. 2008)

1. Verification of heterogeneous systems : CM,…
2. Verification of systems with dynamic memory
3. Verification of WSTS

Assessment 2008-2013
(june 2013)

1. CM

2.

3. WSTS

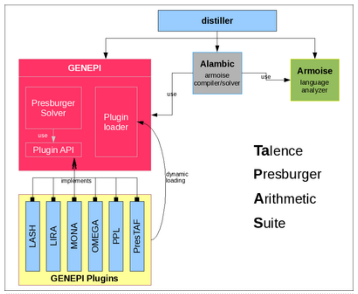
Report of AERES (2008)
versus
our balance (2013)

Report AERES 2009

1. Strengths:
   - Publications, CM
   - FAST

2. To improve
   1. Interaction with program analysis
   2. + cooperation LIAFA
   3. Data dyn.

3. Recommendations
   1. Recrut a CR
   (prog Analysis-dem. Aut.)
   1. Develop FAST



Bilan 2008-2013

1. Strengths :
   - publications, CM
   - WSTS

2. What has been done
   1. More theory WSTS+CM
   2. + cooperation LIAFA (Habermehl, PhD Dahr)

3. What has been done
   1. 2009: Recruitment Laurent Doyen, CR CNRS, on Games
   2. FAST stopped but TAPAS continue

   http://tapas.labri.fr/trac

Objectives and challenges
2013 --> 2017

- **Constat**
  - We have formed brillant researchers in and out of the LSV
  - We inspired fruitful research in France and outside (Oxford, Bruxelles, Vienne, Chennaï, Madrid).

- **Objectives**
  - Strengthen our leadership role in WSTS + CM
  - Recruit a colleague on verification algorithmics
  - Recruit PhD students

- **Challenges**
  - Classify WSTS
  - Complete the theory of complete WSTS
  - Move towards algorithmics (WSTS + CM)

The end

Questions…